

AMENDMENTS TO THE CLAIMS

1. (Original) A system comprising:
operating system providing at least one routine capable of being invoked, and said
operating system operable to collect audit data for invoked operating system routines;
data storage having collected audit data stored thereto in a first format; and
software code executable by at least one processor to receive said collected audit data
and generate output comprising at least a portion of said collected audit data in a desired
format defined by a template, wherein said desired format is different than said first format.
2. (Original) The system of claim 1 wherein said template comprises at least one
constant element.
3. (Original) The system of claim 2 wherein said at least one constant element is
included verbatim in said output.
4. (Original) The system of claim 1 wherein said template comprises at least one
variable element.
5. (Original) The system of claim 4 wherein said at least one variable element
identifies a particular portion of the collected audit data to be included in said output.
6. (Original) The system of claim 5 wherein said at least one variable element
identifies a location within said output at which said particular portion of the collected audit
data is to be arranged.
7. (Original) The system of claim 1 wherein said collected audit data comprises
a record for each invocation of an operating system routine that is included within said
collected audit data, and wherein each record includes at least one type of audit information
relating to execution of an invoked operating system routine.

8. (Original) The system of claim 7 wherein said at least one type of audit information includes at least one type selected from the group consisting of:

user identification, group identification, supplementary group identification, process identification, event identification, event count, event type, date, time, thread identification, system call, capabilities used, object, and result.

9. (Original) The system of claim 7 wherein said template comprises at least one variable element that each identifies a particular type of audit information to be included in said output.

10. (Original) The system of claim 1 wherein said template comprises at least one conditional element.

11. (Original) The system of claim 10 wherein said at least one conditional element dictates that said output is to have a particular format if a condition is satisfied, otherwise said output is to have a different format.

12. (Original) The system of claim 1 wherein said template defines a format selected from the group consisting of:

plain text, markup language, and comma separated format.

13. (Original) The system of claim 1 wherein said operating system comprises a kernel-level audit device driver for collecting said audit data.

14. (Original) A computer program product for generating audit data in a desired format, said audit data relating to execution of a routine, said computer program product comprising a computer-readable storage medium having computer-readable program code embodied in said medium, said computer readable program code comprising:

code executable to access audit data stored in a data storage device, wherein said audit data comprises information relating to execution of at least one invoked routine;

code executable to access an audit transformation template; and

code executable to generate output comprising at least a portion of said collected audit data, said output having a format defined by said audit transformation template.

15. (Original) The computer program product of claim 14 wherein said audit data is collected by an operating system.

16. (Original) The computer program product of claim 14 wherein said at least one routine includes at least one invoked operating system routine.

17. (Original) The computer program product of claim 16 wherein said at least one invoked operating system routine is invoked by an application via system call.

18. (Original) The computer program product of claim 16 wherein said at least one invoked operating system routine is invoked via user command.

19. (Original) The computer program product of claim 14 wherein said audit transformation template comprises at least one constant element that is included verbatim in said output.

20. (Original) The computer program product of claim 14 wherein said template comprises at least one variable elements.

21. (Original) The computer program product of claim 20 wherein said collected audit data comprises a record for each invocation of an operating system routine that is included within said collected audit data, and wherein each record includes at least one type of audit information relating to execution of an invoked operating system routine.

22. (Original) The computer program product of claim 21 wherein said at least one type of audit information includes at least one type selected from the group consisting of: user identification, group identification, supplementary group identification, process identification, event identification, event count, event type, date, time, thread identification, system call, capabilities used, object, and result.

23. (Original) The computer program product of claim 22 wherein said audit data comprises multiple ones of said record, further comprising:

code executable to sort at least a portion of the multiple records based on at least one of said types of audit information.

24. (Original) The computer program product of claim 21 wherein said at least one variable element each identify a particular type of audit information to be included in said output.

25. (Original) The computer program product of claim 14 wherein said template comprises at least one conditional element, and wherein said conditional element dictates that said output is to have a first format if a condition is satisfied and have a different format if said condition is not satisfied.

26. (Original) A method of generating an output that includes collected audit data therein and has a desired format, said method comprising the steps of:
collecting audit data relating to the execution of one or more invoked routines;
storing said collected audit data to a data storage device;
accessing said collected audit data;
accessing an audit transformation template that defines a desired format; and
generating an output that includes at least a portion of said collected audit data,
wherein said output comprises said desired format as defined by said audit transformation template.

27. (Original) The method of claim 26 wherein said audit data comprises information about at least one invoked operating system routine.

28. (Currently Amended) The method of claim 26 further comprising: ~~the step of:~~
creating, by a user, receiving input from a user for creating said audit transformation template.

29. (Original) The method of claim 26 wherein said audit transformation template comprises at least one constant element that is included verbatim in said output.

30. (Original) The method of claim 26 wherein said audit transformation template comprises at least one variable element.

31. (Original) The method of claim 30 wherein said at least one variable element identifies a particular type of audit information from said collected audit data to be included in said output.

32. (Original) The method of claim 31 wherein said particular type of audit information includes at least one type selected from the group consisting of:

user identification, group identification, supplementary group identification, process identification, event identification, event count, event type, date, time, thread identification, system call, capabilities used, object, and result.

33. (Original) The method of claim 26 further comprising the step of: presenting said output to a user.

34. (Original) The method of claim 26 further comprising the step of: storing said output to a file.

35. (Original) The method of claim 26 further comprising the step of: inputting said output to an application for processing by said application.

36. (Original) The method of claim 26 further comprising the step of: sorting said collected audit data based at least in part on at least one type of audit information included therein.

37. (Original) A library of software functions stored to a computer-readable medium comprising:

function executable to access collected audit data, wherein said audit data comprises information about at least one invoked routine of said operating system;

function executable to access a template defining an output format; and

function executable to generate output comprising at least a portion of said collected audit data, wherein said output has a format defined by said template.

38. (Original) The library of claim 37 wherein said function executable to access collected audit data, said function executable to access a template, and said function executable to generate output are distinct functions.

39. (Original) The library of claim 37 wherein said function executable to access collected audit data, said function executable to access a template, and said function executable to generate output are included within a common function.

40. (New) The system of claim 1 wherein said generated output comprises presentation output.

41. (New) The system of claim 40 wherein said presentation output comprises at least one selected from the group consisting of:

presentation output to a display, and presentation output to a printer.

42. (New) The system of claim 40 wherein said presentation output comprises at least one selected from the group consisting of:

presentation output by a browser, presentation output by a spreadsheet program, and presentation output by an application program.

43. (New) The system of claim 1 further comprising:

user interface for receiving from a user input defining said template.

44. (New) The computer program product of claim 14 wherein said code executable to generate output comprises:

code executable to generate presentation output.

45. (New) The computer program product of claim 44 wherein said presentation output comprises at least one selected from the group consisting of:

presentation output to a display, and presentation output to a printer.

46. (New) The computer program product of claim 44 wherein said presentation output comprises at least one selected from the group consisting of:

presentation output by a browser, presentation output by a spreadsheet program, and presentation output by an application program.

47. (New) The computer program product of claim 14 further comprising:

code executable to receive from a user input defining said audit transformation template;

48. (New) The method of claim 26 wherein said generating an output comprises: generating an output presentation.

49. (New) The method of claim 48 wherein said output presentation comprises at least one selected from the group consisting of:

output presentation to a display, and output presentation to a printer.

50. (New) The method of claim 49 wherein said output presentation comprises at least one selected from the group consisting of:

output presentation by a browser, output presentation by a spreadsheet program, and output presentation by an application program.

51. (New) The library of claim 37 wherein said function executable to generate output comprises:

function executable to generate output presentation.

52. (New) The library of claim 51 wherein said output presentation comprises at least one selected from the group consisting of:

output presentation to a display, and output presentation to a printer.

53. (New) The library of claim 52 wherein said output presentation comprises at least one selected from the group consisting of:

output presentation by a browser, output presentation by a spreadsheet program, and output presentation by an application program.

54. (New) A method of generating an output presentation that includes collected audit data therein and has a desired format, said method comprising the steps of:

receiving input defining an audit transformation template that defines a desired format for said output presentation;

collecting audit data relating to the execution of one or more invoked routines;

storing said collected audit data to a data storage device;

accessing said collected audit data;

accessing said audit transformation template that defines a desired format; and

generating said output presentation that includes at least a portion of said collected audit data, wherein said output presentation comprises said desired format as defined by said audit transformation template.